70-643^{Q&As}

Windows Server 2008 Applications Infrastructure, Configuring

Pass Microsoft 70-643 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.pass4itsure.com/70-643.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Microsoft Official Exam Center

⚙ **Instant Download** After Purchase

⚙ **100% Money Back** Guarantee

⚙ **365 Days** Free Update

⚙ **800,000+** Satisfied Customers

QUESTION 1

Your network contains two servers that have the Hyper-V server role installed.

You install the Failover Clustering feature on both servers. You add both servers as nodes in the cluster.

You need to ensure that you can perform live migrations of individual virtual machines (VMs) between the nodes.

The solution must minimize the number of volumes required to host the VMs.

What should you do first?

A. From Failover Cluster Manager, enable Cluster Shared Volumes.

B. From Failover Cluster Manager, modify the quorum settings of the cluster.

C. From Hyper-V Manager on each server, modify the default location for the virtual hard disks (VHDs).

D. From Hyper-V Manager on each server, modify the default location for the virtual machine configuration files.

Correct Answer: A

Cluster Shared Volumes, a feature available with some versions of failover clustering, simplifies the configuration and management of clustered virtual machines.

With Cluster Shared Volumes, multiple clustered virtual machines can use the same LUN (disk) while still being able to fail over (or move from node to node) independently of one another.

Note In Windows ServerR 2008 R2, the Cluster Shared Volumes feature included in failover clustering is only supported for use with the Hyper-V server role. The creation, reproduction, and storage of files on Cluster Shared Volumes that

were not created for the Hyper-V role, including any user or application data stored under the ClusterStorage folder of the system drive on every node, are not supported and may result in unpredictable behavior, including data corruption or

data loss on these shared volumes. Only files that are created for the Hyper-V role can be stored on Cluster Shared Volumes. An example of a file type that is created for the Hyper-V role is a Virtual Hard Disk (VHD) file.

Before installing any software utility that might access files stored on Cluster Shared Volumes (for example, an antivirus or backup solution), review the documentation or check with the vendor to verify that the application or utility is

compatible with Cluster Shared Volumes.

Overview of Cluster Shared Volumes

Cluster Shared Volumes is available in versions of Windows ServerR 2008 R2 and of MicrosoftR Hyper-VTM Server 2008 R2 that include the Failover Clustering feature. Volumes that are configured as Cluster Shared Volumes can be

accessed by all nodes of a failover cluster. Each node can open and manage files on the volumes. Therefore, different nodes can host different virtual machines that all have files on the same volume.

This design has many advantages, including the following:

Easier storage management: When virtual machines share volumes, fewer LUNs need to be configured and managed to host the same number of virtual machines. Independent failover of virtual machines : Although multiple virtual

machines

are sharing the same volume, each virtual machine can fail over, or be moved or migrated, independently of other virtual machines. No drive letter restrictions: Cluster Shared Volumes do not need to be assigned a drive letter, so you are not

restricted by the number of available drive letters, and you do not have to manage volumes using GUIDs.

Enhanced availability: The Cluster Shared Volumes feature is designed to detect and handle many problems that would otherwise cause the storage to be unavailable to virtual machines. This includes detecting and handling storage

connection problems (Cluster Shared Volumes reroutes the storage access through another node).

Efficient use of storage: You can make better use of disk space, because you do not need to place each Virtual Hard Disk (VHD) file on a separate disk with extra free space set aside just for that VHD file. Instead, the free space on a Cluster

Shared Volume can be used by any VHD file on that LUN. This reduces the total amount of space that must be set aside for expansion, and simplifies capacity planning

Source: http://technet.microsoft.com/en-us/library/dd630633(WS.10).aspx

QUESTION 2

Your network contains a server named Server1 that runs Windows Server 2008 R2 Service Pack 1 (SP1).

You install the SMTP Server feature on Server1.

You verify that Server1 receives email messages.

You restart Server1.

You discover that Server1 no longer receives email messages. You need to ensure that Server1 can receive email messages after the restart.

What should you do on Server1?

A. From Internet Information Services (IIS) 6.0 Manager, configure the Relay Restrictions settings

B. From the Services console, modify the startup type of the Message Queuing feature.

C. From Internet Information Services (IIS) 6.0 Manager, configure the Security settings.

D. From the Services console, modify the startup type of the Simple Mail Transfer Protocol (SMTP) service.
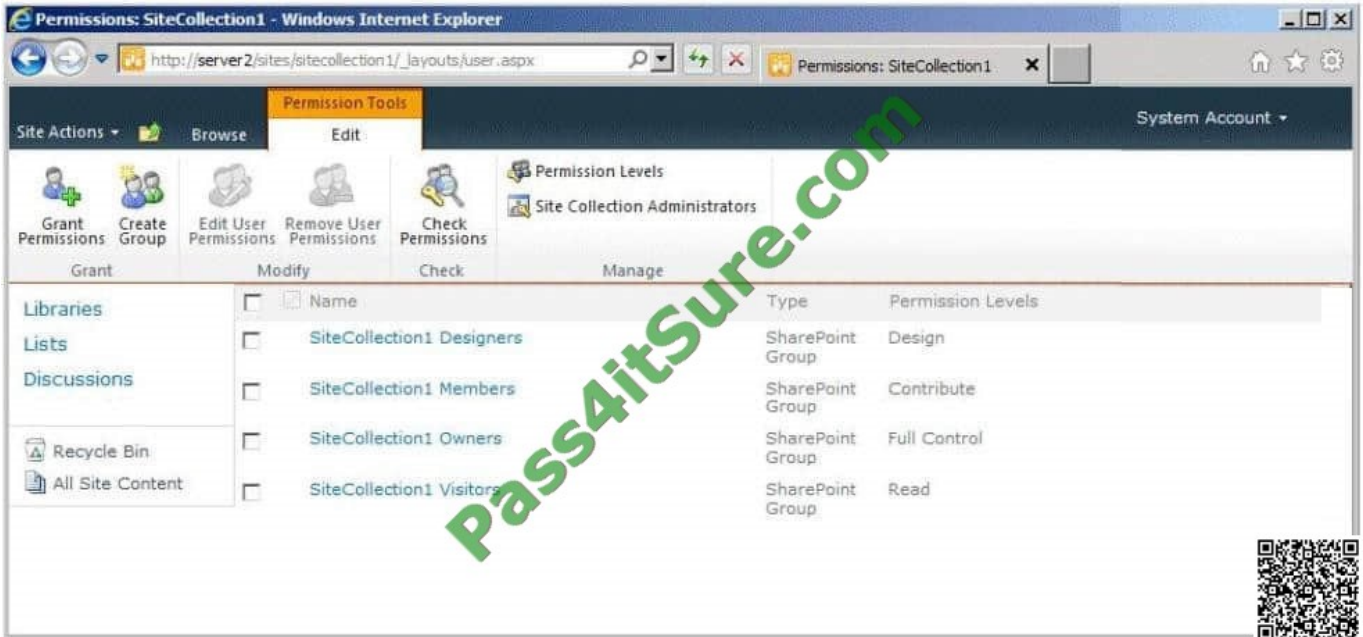
Correct Answer: D

QUESTION 3

Your network contains a server named Server2 that has Microsoft SharePoint Foundation 2010 Service Pack 1 (SP1) installed.

You have a site collection named SiteCollection1.

The groups in SiteCollection1 are shown in the exhibit. (Click the Exhibit button.)

You need to ensure that a user named User1 can create and delete lists in SiteCollection1. The solution must minimize the number of permissions assigned to User1.

To which group should add User1?

A. SiteCollection1 Visitors

B. SiteCollection1 Owners

C. SiteCollection1 Designers

D. SiteCollection1 Members

Correct Answer: D

Default permission levels Permission levels are collections of permissions that allow users to perform a set of related tasks. SharePoint Foundation 2010 includes five permission levels by default. You can customize the permissions available in these permission levels (except for the Limited Access and Full Control permission levels), or you can create customized permission levels that contain only the permissions you need.

The following table lists the default permission levels for team sites in SharePoint Foundation 2010.

Permission level	Description	Permissions included by default
Limited Access	Allows access to shared resources in the Web site so that the users can access an item within the site. Designed to be combined with fine-grained permissions to give users access to a specific list, document library, folder, list item, or document, without giving them access to the entire site. Cannot be customized or deleted.	View Application Pages Browse User Information Use Remote Interfaces Use Client Integration Features Open
Read	View pages, list items and download documents.	Limited Access permissions, plus: View Items Open Items View Versions Create Alerts Use Self-Service Site Creation View Pages
Contribute	View, add, update, and delete items in the existing lists and document libraries.	Read permissions, plus: Add Items Edit Items Delete Items Delete Versions Browse Directories Edit Personal User Information Manage Personal Views Add/Remove Personal Web Parts Update Personal Web Parts
Design	View, add, update, delete, approve, and customize items or pages in the Web site.	Approve permissions, plus: Manage Lists Add and Customize Pages Apply Themes and Borders Apply Style Sheets
Full Control	Allows full control of the scope.	All permissions

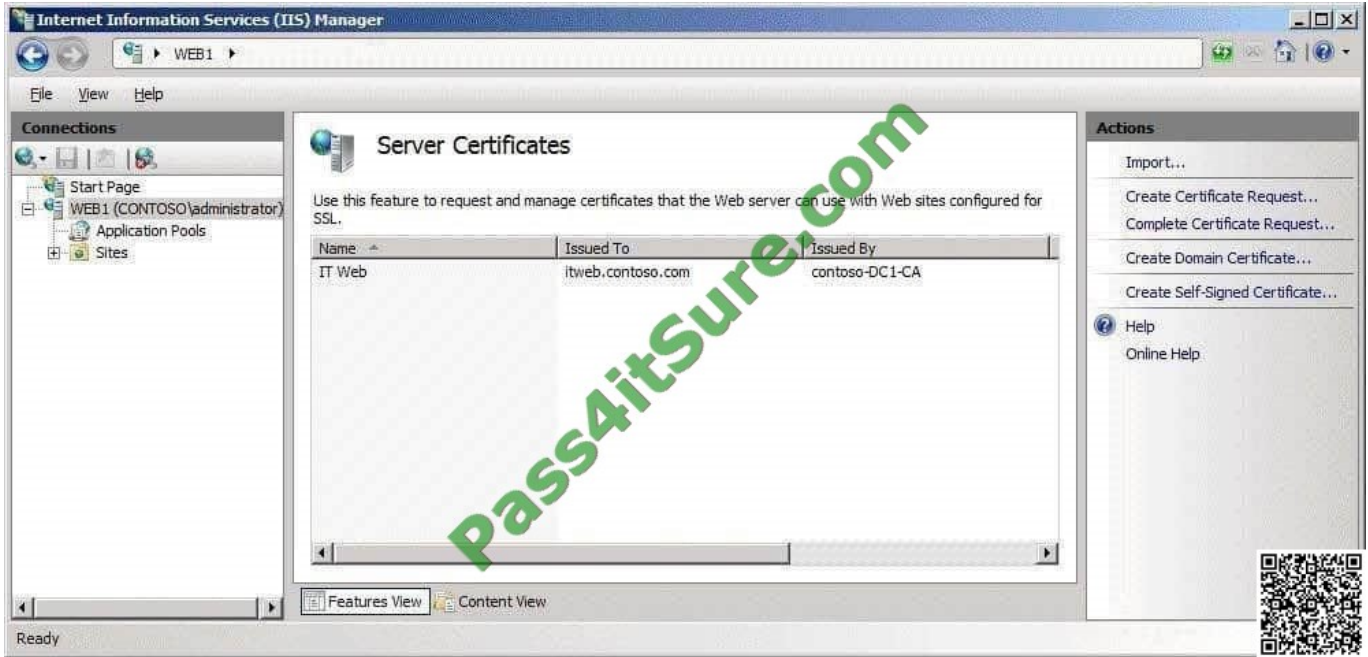Source: http://technet.microsoft.com/en-us/library/cc288074.aspx

QUESTION 4

Your network contains a server named Web1 that runs Windows Server 2008 R2. Web1 has the Web Server (IIS) role installed.

Web1 hosts a Web site that is accessed by using the URL http://itweb.contoso.com. The server certificates for Web1 are shown in the exhibit. (Click the Exhibit tton.)

When you attempt to configure the SSL Settings for the Web site, you discover that the Require SSL option is unavailable. You need to ensure that you can require SSL for the Web site. What should you do?

A. Run iisreset.exe /force.

B. Configure the bindings for the Web site.

C. Request a new domain certificate and specify Web1 as the common name.

D. Request a self-signed certificate and specify itweb.contoso.com as the friendly name.

Correct Answer: B

So one needs to add a Site Binding to HTTPS:

QUESTION 5

Your company has an Active Directory domain. The company runs Remote Desktop Services.

Standard users who connect to the Remote Desktop Session Host Server are in the TSUsers organizational unit (OU). Administrative users are in the TSAdmins OU. No other users connect to the Remote Desktop Session Host Server.

You need to ensure that only members of OU1 can run the Remote Desktop Protocol files.

What should you do?

A. Create a Group Policy object (GPO) that configures the Allow .rdp files from unknown publishers policy setting in the Remote Desktop Client Connection template to Disabled. Apply the GPO to the TSUsers OU.

B. Create a Group Policy object (GPO) that configures the Allow .rdp files from valid publishers and users default .rdp settings policy setting in the Remote Desktop Client Connection template to Disabled. Apply the GPO to the TSUsers OU.

C. Create a Group Policy object (GPO) that configures the Allow .rdp files from valid publishers and users default .rdp settings policy setting in the Remote Desktop Client Connection template to Enabled. Apply the GPO to the TSAdmins OU.

D. Create a Group Policy object (GPO) that configures the Specify SHA1 thumbprints of certificates representing trusted .rdp publishers policy setting in the Remote Desktop Client Connection template to Enabled. Apply the GPO to the TSAdmins OU.

Correct Answer: C

To ensure that only members of the TermSerAdmin OU can run the Remote Desktop Protocol files, you need to enable the Allow .rdp files from valid publishers and users default .rdp settings policy setting in the Remote Desktop Client Connection template.

This policy setting allows you to specify whether users can run Remote Desktop Protocol (.rdp) files from a publisher that signed the file with a valid certificate. A valid certificate is one issued by an authority recognized by the client, such as the issuers in the client\\'s Third-Party Root Certification Authorities certificate store.

This policy setting also controls whether the user can start an RDP session by using default .rdp settings (for example, when a user directly opens the Remote Desktop Connection [RDC] client without specifying an .rdp file). If you enable this policy setting, users can run .rdp files that are signed with a valid certificate.

Users can also start an RDP session with default .rdp settings by directly opening the RDC client. When a user starts an

RDP session, the user is asked to confirm whether they want to connect.

If you disable this policy setting, users cannot run .rdp files that are signed with a valid certificate. Additionally, users cannot start an RDP session by directly opening the RDC client and specifying the remote computer name. When a user tries to start an RDP session, the user receives a message that the publisher has been blocked

Reference: Remote Desktop Connection Client
http://technet2.microsoft.com/windowsserver2008/en/library/76fb7e12-b823-429b-9887-05dc70d28d0c1033.mspx?mfr=true

---

70-643 PDF Dumps   70-643 VCE Dumps   70-643 Exam Questions